IN THE UNITED STATES PATENT and TRADEMARK OFFICE

Inventors:	Yigal Mordechai Edery, Nimrod Itzhak Vered, David R Kroll, Shlomo Touboul	Control No.: Unassigned
Patent No.:	8,079,086	
Issue Date:	Dec. 13, 2011	
Filing Date:	May 26, 2009	
Title:	MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS	

Mail Stop Ex Parte Reexam
Central Reexamination Unit
Office of Patent Legal Administration
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

ATTACHMENT TO REQUEST FOR EX-PARTE REEXAMINATION (FORM PTO-SB/57; PTO-1465) PROVIDING INFORMATION ON U.S. PATENT NO. 8,079,086

Reexamination under 35 U.S.C. §§ 302-307 and 37 C.F.R. § 1.510 is respectfully requested of United States Patent No. 8,079,086 ("the Edery 086 patent"), which was filed on May 26, 2009 and issued on December 13, 2011. The Edery 086 patent is enforceable and reexamination is appropriate under 37 C.F.R. § 1.510(a). Currently, the Edery 086 patent is being asserted in the patent infringement lawsuits styled *Finjan, Inc. v. FireEye, Inc.*, 13-cv-3133 (N.D. Cal.), filed on July 8, 2013 and *Finjan, Inc. v. Proofpoint et al.*, 13-cv-5808 (N.D. Cal.), filed on December 16, 2013.

I. CLAIMS FOR WHICH REEXAMINATION IS REQUESTED

Reexamination is requested of claims 1-8, 17-23, 31, 32, 35, 36, 39 and 41 of the Edery 086 patent.

II. CITATION OF PRIOR ART

The Edery 086 patent was filed on May 26, 2009 as application No. 12/471,942 ("the 942 application"). It is a continuation of and claims priority to U.S. Patent No. 7,613,926 to Edery ("Edery 926"), filed on March 7, 2006, which is a continuation of U.S. Patent No. 7,058,822 to

Edery ("Edery 822"), which was filed on May 17, 2001. Reexamination of the Edery 822 patent was instituted on December 5, 2013 as reexamination control number 90/013,017. Claims 1-8 and 16-27 of the Edery 822 patent are currently subject to reexamination.

Requester seeks reexamination of the Edery 086 patent in light of the combination of U.S. Patent No. 5,983,348 to Ji (the "Ji patent") and PCT application publication number WO 98/21683 to Touboul (the "Touboul Application"). The Ji patent was filed on September 10, 1997 and issued on November 9, 1999. The Touboul Application was filed on November 6, 1997 and published on May 22, 1998. Thus, the Ji patent in combination with the Touboul Application is prior art to the Edery 086 patent under 35 U.S.C. § 103(a). The Touboul Application was not considered during the examination of the Edery 086 patent, either alone or in combination with the Ji patent.[1] Because the combination of the Ji patent and the Touboul Application was not previously considered by the Patent Office, this combination provides a new ground for examination. As discussed below, the new ground for examination coupled with the disclosure of all elements of claims 1-8, 17-23, 31, 32, 35, 36, 39 and 41 by the combination of the Ji patent and the Touboul Application constitutes a substantial new question of patentability.

III. STATEMENT POINTING OUT SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

The combination of the Ji patent and Touboul Application constitutes a substantial new question of patentability. All elements of the claims for which reexamination is requested are clearly present in that combination of references, and that combination of references was not previously considered by the Patent Office.

On October 7, 2013, Requestor initially sought reexamination of the Edery 086 patent based on combination of the Ji patent and the Touboul 194 patent. That reexamination request was given reexamination control number 90/013,015 ("the 015 reexamination request"). On November 19, 2013, Examiner Cabrera denied the reexamination request, finding that the prior art combination of the Ji patent and the Touboul 194 patent did not raise a substantial new question of patentability. 015 reexamination request, Nov. 19, 2013 Order at 12. Examiner

[1] A related patent (U.S. Patent No. 6,092,194 to Touboul (the "Touboul 194 patent")) was cited during the examination of the Edery 086 patent. Applicants terminally disclaimed the Touboul 194 patent during prosecution. On December 21, 2012, the Touboul 194 patent was found invalid by a civil jury in the United States District Court for the District of Delaware in the lawsuit styled *Finjan, Inc. v. Symantec Corp., et. al*, 10-cv-00593 GMS.

Cabrera concluded that the original examination of the Edery 086 patent determined that: (1) the Ji patent's "instrumenting" was not the claimed step of "appending a representation of the Downloadable security profile data to the Downloadable"; and (2) the Ji patent's transmission of an "instrumented" applet was not the claimed step of "transmitting the Downloadable and a representation of the Downloadable security profile data…." Examiner Cabrera therefore concluded that the Requestor did not overcome these failings because "the request relies on the 'instrumented applet' for the limitation 'the Downloadable and a representation of the Downloadable security profile data." *Id.* at 10-11 (emphasis in original). In contrast to this finding, the instant request does not rely on the Ji patent in the manner rejected in the 015 reexamination request. This request relies on the Downloadable security profile data disclosed in the Touboul Application in combination with the Ji patent's disclosure of appending a security monitoring package—not the instrumentation functionality disclosed in the Ji patent.

Requestor has filed the instant reexamination request to clarify that the combination of the Ji patent and the Touboul Application (as distinct from the Touboul 194 patent) discloses the claim limitations of the Edery 086 patent including the above noted limitations reciting (1) "appending a representation of the Downloadable security profile data to the Downloadable" and (2) "transmitting the Downloadable and a representation of the Downloadable security profile data." The instant request sets forth below the disclosure of the "appending" and "transmitting" claim elements by the appending of a security monitoring package to the Downloadable with subsequent transmission of the security package and the Downloadable to the client, as disclosed in the Ji patent (e.g., Ji at 3:45-50), and the "representation of the Downloadable security profile data" claim element disclosed in the Touboul Application (e.g., Touboul Application at 17:1-2). Notably, the instant request does not rely on the instrumentation of suspicious computer operations disclosed in the Ji patent (e.g., at 5:16-6:37). The instant request therefore overcomes the purported deficiencies of the prior 015 reexamination request.

Thus, the Ji patent in combination with the Touboul Application establishes a substantial new question of patentability of claims 1-8, 17-23, 31, 32, 35, 36, 39 and 41 of the Edery 086 patent. The substantial new question of patentability meets the legal standard for ordering *ex parte* reexamination as set forth in the MPEP § 2216:

> It must first be demonstrated that a patent or printed publication that is relied upon in a proposed rejection presents a new, non-cumulative technological teaching that was not previously

> considered and discussed on the record during the prosecution of the application that resulted in the patent for which reexamination is requested, and during the prosecution of any other prior proceeding involving the patent for which reexamination is requested.

The combination of the Ji patent and the Touboul Application discloses all elements of the claims of the Edery 086 patent for which reexamination is requested. Therefore, the Office should grant this request.

A. Background of the Edery 086 Patent

The Edery 086 patent relates to protection systems and methods capable of protecting network accessible devices or processes from malicious operations. The disclosed embodiments determine whether information received from a third party includes executable code. Furthermore, the embodiments disclosed in the Edery 086 patent contemplate "delivering static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables." Edery 086 at Col. 2, lines 55-59. The embodiments further disclose causing the mobile protection code to be executed within the destination, which could include a web browser, in a manner that enables the Downloadable operations to be detected, intercepted, or further responded to via the various protected operations. Edery 086 at Col. 3, lines 32-50.

The methods disclosed in independent claims 1, 17, 31, 35, 39 and 41 are depicted in Figure 9 of the Edery 086 patent:

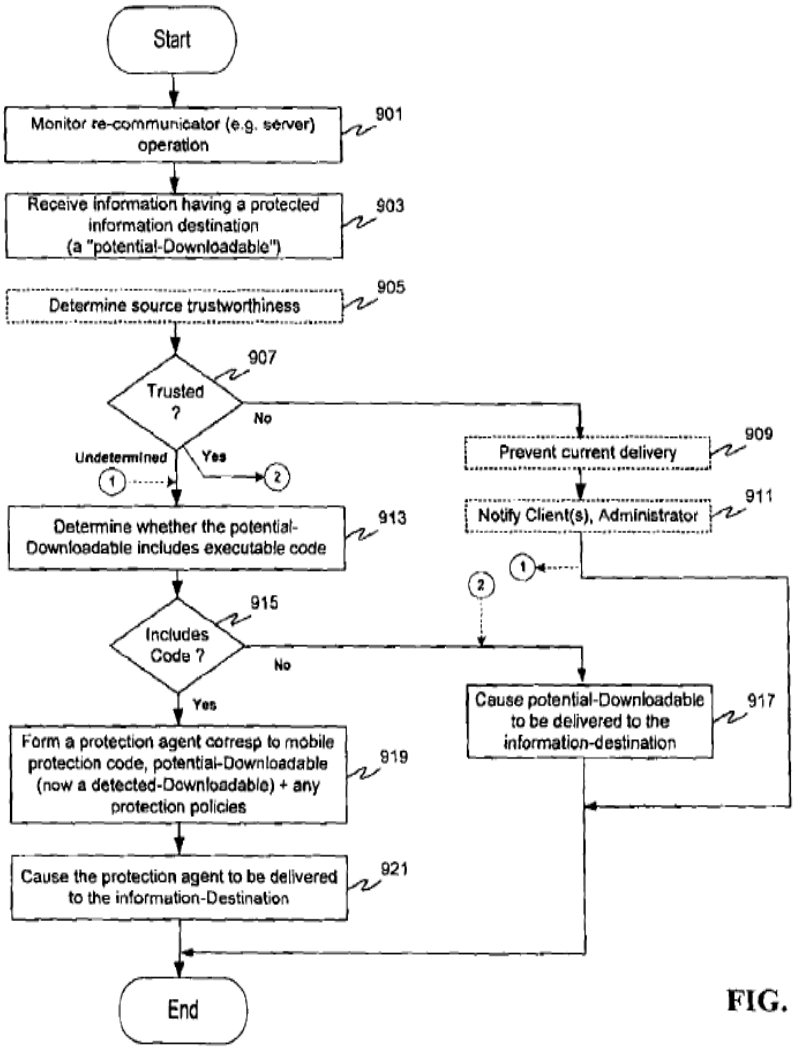


FIG. 9

In addition to the aforementioned embodiments, the method set forth in claim 1 involves a computer receiving downloadable information, deriving security profile data for the Downloadable and appending a representation of the Downloadable security data to the Downloadable to generate an appended Downloadable before transmitting the appended Downloadable to a third device, such as a computer.

B. The Examination of the Edery 086 Patent

The 942 application, which issued as the Edery 086 patent, was filed on May 26, 2009. With that filing, the applicants filed a preliminary amendment adding claims of priority to (1) the Edery 822 patent, (2) U.S. Patent No. 6,804,780 ("Touboul 780"), (3) the Touboul 194 patent, and (4) U.S. Patent No. 6,480,962[2] ("Touboul 962"). May 26, 2009 Preliminary Amendment at

[2] On December 21, 2012, the Touboul 962 patent was found invalid by a civil jury in the United

p. 2. The preliminary amendment also designated the 942 application as a continuation of application U.S. Serial No. 11/370,114 (now Edery 926), which was a continuation of U.S. Serial No. 09/861,229, which matured into Edery 822. *Id*. at pp. 2-3. The preliminary amendment additionally cancelled claims 1-76 and added new claims 77-136. *Id*. at pp. 3-16.

In the preliminary amendment, the applicants addressed prior rejections based on the Ji patent that were set forth in an Office Action in the co-pending parent application No. 11/370,114. The applicants argued that the Ji patent, filed on September 10, 1997, was inadmissible prior art. *Id*. at p. 18. The applicants contended that the 942 application and its pending claims were supported by U.S. provisional application No. 60/030,639 and were entitled to a November 8, 1996 priority date. *Id*. at p. 19. However, as explained in Section III. D. below, the applicants dropped this argument and did not refute the examiner's assertion that the 942 application could not claim priority to this provisional application.

The applicants then argued that the added claims were not anticipated or rendered obvious by the Ji patent because: "(i) Ji does not disclose a Downloadable security profile database, and (ii) Ji does not disclose appending a security profile of a Downloadable to a Downloadable." *Id*. at p. 19. Therefore, the applicants limited the alleged novelty of the 942 application to these two discrete points. The applicants described their invention as "relat[ing] to a Downloadable security scanner that operates by deriving or retrieving a security profile for a Downloading, and transmitting the Downloadable and a representation of the security profile to a receiver computer." *Id*. The applicants further stated that: "The security profile [itself] includes a list of suspicious computer operations that may be performed by the Downloadable," and "[t]he representation of the security profile may be appended to the Downloadable." *Id*. The applicants also stated that the receiver computer in turn reviews the security profile and decides based on the security profile whether or not to execute the Downloadable and, "if so, whether or not to execute the Downloadable in a controlled manner or environment." *Id*.

The applicants stated that the Ji patent, on the other hand, "describes an applet security scanner that operates by identifying suspicious function calls in an applet, and inserting a first instruction sequence, before a suspicious function call, and inserting a second instruction

---

States District Court for the District of Delaware in the lawsuit styled 10-cv-00593 GMS. Additionally, the '962 patent has been invalidated by the Patent Office. The Patent Office has closed prosecution rejecting claims 1-55 as anticipated and/or obvious in *inter partes reexamination* Control No. 95/001,836 action closing prosecution pursuant to MPEP § 2671.02.

sequence, after the suspicious function call." *Id*. at pp. 19-20. The applicants argued that, given their characterization of the Ji patent, the Ji patent did not disclose a Downloadable security profile database. *Id*. The applicants also argued that "Ji does not disclose appending a security profile of a Downloadable to a Downloadable." *Id*. at 21. The applicants attempted to distinguish the Ji patent by arguing that it "discloses alteration of a downloadable, referred to in Ji as '*instrumentation*', to disable suspicious operations." *Id*. (emphasis in original). The applicants described their claimed invention as:

> [A]ppend[ing] a list of suspicious operations in the form of a security profile to a Downloadable, for a receiver thereof to decide how to respond thereto. One receiver may allow the Downloadable to execute, in response to the security profile, yet another receiver may block it.

Id. To attempt to distinguish the Ji patent, the applicants argued that "[w]hereas Ji takes an instrumentation action to disable suspicious operations, the claimed invention provides a report about the suspicious operations." *Id*. The applicants then argued that the Ji patent was distinguishable from the claims of the 942 application for the reasons set forth above. *Id*. at pp. 21-27.

On September 20, 2010, the Patent Office issued an Office Action rejecting all pending claims. The Office Action included many rejections, including the rejection of claims 77-136 under 35 U.S.C. § 102(e) as anticipated by the Ji patent. Regarding claim 77, the examiner stated that the Ji patent teaches "a computer-based method, comprising the steps of receiving an incoming Downloadable; deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and storing the Downloadable security profile data in a database (col. 3, lines 32-56 and col. 6, lines 38-51)." *Id*. at pp. 6-7. The examiner then described how each of the pending claims were anticipated by the Ji patent. *Id*. at 7-13.

On December 20, 2010, the applicants amended claims 113, 114, 116, 117, 120, 121, 123 and 124 "to more properly claim the present invention" without allegedly introducing new matter. Dec. 20, 2010 Amendment at p. 16. The applicants also argued that the examiner "did not consider applicants' arguments" from their May 26, 2009 preliminary amendment. *Id*. at p. 17. The applicants then repeated their arguments from the May 26, 2009 preliminary amendment that the pending claims were allowable over the Ji patent. *Id*. at pp. 17-26.

On June 15, 2011, the examiner issued a Final Office Action rejecting all of the pending claims. The examiner found that the applicants' prior arguments were "not persuasive." June 15, 2011 Office Action at p. 2. The examiner disagreed that U.S. provisional application Serial No. 60/030,639 provided support for the claims in the 942 application and requested a specific showing from the provisional application to prove support for the priority date of November 8, 1996. *Id*. The June 15, 2011 Office Action listed the priority date of the 942 application as November 6, 1997, but provided no analysis or support for that date. This alleged priority date is incorrect for the reasons set forth in Section III.D.

In response to the applicants' prior arguments, the examiner noted that the features relied upon by the applicants to distinguish the prior art were not recited in rejected claims 77-94. The examiner stated that "Ji discloses of a downloadable security profile database, the teachings recite of sending reports back to a server (containing a database) which include a list of suspicious operations that may be attempted by the downloadable, see column 6, lines 38-51." *Id*. at 3.

In one rejection, claims 77-94 were rejected under 35 U.S.C. 102(e) as being anticipated by the Ji patent. The examiner noted:

> As per claim 77, it is taught of a computer based method, comprising the steps of receiving an incoming Downloadable; deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and storing the Downloadable security profile data in a database (col. 3, lines 32-56 and col. 6, lines 38-51).

Id. at p. 7. The examiner identified similar reasons and citations in the Ji patent, demonstrating how the Ji patent anticipated claims 77-94 of the 942 application. *Id*. at pp. 7-8. The examiner indicated that pending claims 95-136 were allowable if the rejections under obvious-type double patenting were overcome.

On July 19, 2011, the applicants responded by cancelling claims 77-94 and filing a terminal disclaimer to overcome pending obvious-type double patenting rejections. July 11, 2011 Response at p. 2. The applicants did not, however, address the examiner's conclusion that the 942 application could not claim priority to U.S. provisional application Serial No. 60/030,639.

On August 10, 2011 the examiner issued a Notice of Allowance. On December 13, 2011, the 942 application issued as the Edery 086 patent.

C. SNQP – The Ji Patent In View of the Touboul Application raises a SNQP as to Claims 1-8, 17-23, 31, 32, 35, 36, 39, and 41 under 37 CFR 1.510(b)(1)

The combination of the Ji patent and Touboul Application constitutes a substantial new question of patentability. All elements of the claims for which reexamination is requested are present in that combination of references, and that combination of references was not previously considered by the Patent Office.

Under the *KSR International Co. v. Teleflex Inc.* obviousness standard,[3] the teachings from the Ji patent and the Touboul Application are properly combinable and representative of the obvious body of knowledge within the grasp of the average practitioner skilled in the art of computer network protection. One of ordinary skill in the art would be motivated to combine the Ji patent and the Touboul Application because they are directed to very similar technology. *See* Ji at 1:66-2:42; Touboul Application at 1:5-3:12.

Requestor's prior request for reexamination did not rely on the combination of the Ji patent and the Touboul Application. As noted above, Examiner Cabrera in the 015 reexamination request concluded that "the request relies on the teaching of 'instrumenting' the applet or Java class files for the limitation '*appending a representation of the Downloadable security profile data to the Downloadable*.'" 015 reexamination at 10-11 (emphasis in original). Examiner Cabrera then concluded that a substantial new question of patentability was not raised because the original examination of the Edery 086 patent determined that: (1) the Ji patent's "instrumenting" was not the claimed step of "appending a representation of the Downloadable security profile data to the Downloadable"; and (2) the Ji patent's transmission of an "instrumented" applet was not the claimed step of "transmitting the Downloadable and a representation of the Downloadable security profile data."

The instant request highlights the substantial new question of patentability in light of the combination of the Ji patent with the Touboul Application. Specifically addressing the

---

[3] In *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 415 (2007), the Supreme Court "beg[a]n by rejecting the rigid approach of the Court of Appeals (i.e., requiring satisfaction of the "teaching, suggestion, motivation" (TSM) test) to show an invention would have been obvious (and is therefore unpatentable). Returning to its own nonobviousness cases, the Court held that "the [nonobviousness] analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id*. at 418 (emphasis added).

examiner's points (1) and (2) listed in the preceding paragraph, and as discussed below in more detail, the instant request sets forth the combination of the "appending" and "transmitting" of Downloadable claim elements in the Ji patent—not the Ji patent's instrumenting functionality—with "the representation of the Downloadable security profile data" claim element in the Touboul Application (at 9:14-24) that was not previously considered by the Patent Office.

The Touboul Application discloses the representation of the Downloadable security profile data (commonly referred to as the DSP data). Namely, the Touboul Application discusses the method for deriving the DSP data by decomposing the Downloadable's code into DSP data, which, in combination with the Ji reference discussed below, would be appended to the Downloadable. Touboul App. at 17:1-16; Fig. 7; 9:14-24. The Touboul Application sets forth its disclosure of deriving the DSP data in Figure 7:

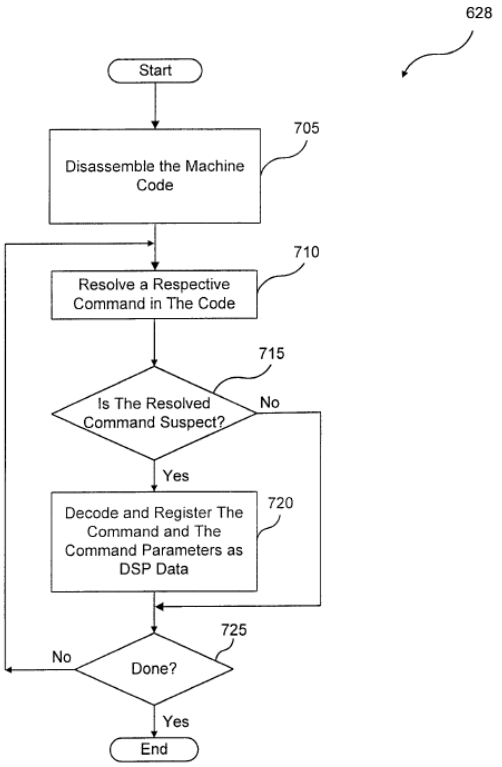


FIG. 7

Touboul App. Fig. 7. And, as discussed below, this is the same downloadable security profile data that applicants argued during prosecution in overcoming other prior art "provides a report about the suspicious operations." Dec. 20, 2010 Response at p. 18-19.

The Ji patent discloses "appending" code to a Downloadable at a server before "transmitting" that Downloadable with the appended code from the server to the intended client

device. Ji at 3:45-50, 6:38-42, 7:41-44, and 8:4-10. As described below, the Ji patent specifically discloses, at the server, appending to the Java applet (the "Downloadable") the security monitoring package:

> More broadly, the present invention is directed to delivering what is referred to as a "live agent" (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions.

Ji at 3:45-50 (emphasis added). *See also* Ji at 8:4-10 (server sends to the client a new JAR file containing a security monitoring package and the applet); Ji at 7:41-44 (server sends monitoring package and applet to the client). The security monitoring package generated for a downloadable, unlike the instrumented applet relied on in the 015 reexamination, is comprised of the security policies and security checker code. Ji at 7:44-64. Therefore, the Ji patent discloses the appending of a security monitoring package to an applet.

A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent showed awareness of Finjan Software, Ltd., the Touboul Application's applicant and assignee, by specifically disclosing Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by these software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, Ltd., a person of ordinary skill in the art would have been motivated to combine the Ji patent with the teachings of Finjan's Touboul Application to provide a solution balancing server-side and client-side activity.

Indeed, during original examination of Edery 086, the discussion regarding this issue focused not on the "appending" functionality but instead on the actions of the "instrumented" code:

> Ji discloses alteration of a Downloadable, referred to in Ji as *"instrumentation"*, to disable suspicious operations (Ji/ col, 3,

> lines 26-31; col 5, lines 1, 2 and 16-43). In distinction, the claimed invention appends a list of suspicious operations in the form of a security profile to a Downloadable, for a receiver thereof to decide how to respond thereto. One receiver may allow the Downloadable to execute, in response to the security profile, yet another receiver may block it. Whereas Ji takes an instrumentation action to disable suspicious operations, the claimed invention provides a report about the suspicious operations.

Dec. 20, 2010 Response at p. 19 (emphasis added). In the applicants' response to the Office Action, they limited their arguments to claiming that the invention was distinct from Ji due to the actions performed by the appended code in response to security threats—not to the act of appending code to the Downloadable or to the transmission of the Downloadable and the appended code. The applicants did not dispute that the Ji patent disclosed the "appending" and "transmitting" elements. Instead, the applicants argued that the claimed invention "provides a report about the suspicious operations," which the applicants argued was not found in Ji (presumably because Ji's instrumented code was not a "representation of the Downloadable security profile"). Dec. 20, 2010 Response at 18-19. As discussed below, the instant request relies on the Touboul Application and its disclosure of DSP data and "provid[ing] a report about the suspicious operations" to be attempted by the Downloadable to satisfy the claim element that the applicants argued was missing from Ji.[4]

---

[4] Requestor is not relying on Ji for purposes of disclosing the "representation of the Downloadable security profile." The Touboul Application provides that disclosure. However, the security monitor package functionality disclosed in the Ji patent (at 7:44-64) is akin to "provid[ing] a report about the suspicious operations" in that it discloses reporting to a user that a security policy violation has occurred:

> The monitor package also creates a unique session upon instantiation. It also contains a security policy checker (supplied by security policy generator component 54) to determine whether the applet being scanned violates the security policy, given the monitoring information.
>
> The security policy generator component 54 generates the security checker code included in the monitor package, from a set of predefined security policies. Different clients, users, and applets may have different security policies. The security policy generator 54 may run on server machine 20 or another computer. In addition, security policies can be configured by an administrator of the system. A simple security policy is to assign different weights to monitored functions and make sure the security weight of a session does not exceed a preset threshold. A more sophisticated security policy checks the file or resource the applet is trying to access at run time and prompts the user whether to allow the access. Hence the

The substantial new question of patentability presented here stems from the combination of the Ji patent's disclosure of "appending" a security monitoring package to a Downloadable and "transmitting" the appended security monitoring package and Downloadable, along with the Touboul Application's disclosure of the derivation and use of the "representation of the Downloadable security profile data"—the same Downloadable security profile data disclosed in the Edery 086 patent. *See* Ji at 3:45-50, 6:38-42, 7:41-44 and 8:4-10; Touboul App. at 5:23-6:6, 6:21-7:6, 7:10-14, 9:11-24 and 17:1-16.

Accordingly, the two claim elements that the applicants argued did not exist in the prior art are clearly disclosed in the combination of the Ji patent and the Touboul Application, and this combination raises a substantial new question of patentability not previously considered by the examiner. *See In re Swanson*, 540 F.3d 1368, 1380 (Fed. Cir. 2008) ("the PTO should evaluate the context in which the reference was previously considered and the scope of the prior consideration and determine whether the reference is now being considered for a substantially different purpose").

The Ji patent discloses the ability to append code (specifically, the monitoring package) to a Downloadable. Accordingly, the examiner's position in the earlier reexamination request is inapposite to and distinct from the arguments presented here. Moreover, as set forth above and in the claim charts below, it would have been obvious to combine the Ji patent's disclosure of the "appending" and "transmitting/transmission" capability with the Touboul Application's disclosure of the "representation of the Downloadable security profile data" to be used in the generation of an appended Downloadable, the transmission of the Downloadable and the representation of the Downloadable security profile data.

D. The Edery 086 Patent Is Not Entitled to a Priority Date From The Alleged Parent Continuation-In-Part Patents.

The Edery 086 patent cannot claim priority to any application filed before the Edery 822 patent's May 17, 2001 filing date. As the MPEP explains, determination of the proper priority date is appropriate as part of a request for *ex parte* reexamination:

> The statement applying the prior art may, where appropriate, point out that claims in the patent for which reexamination is requested are entitled only to the filing date of that patent and not supported

---

> security policy broadly is a state machine to detect security policy violations upon attempted instruction execution.

(emphasis added).

> by an earlier foreign or United States patent application whose filing date is claimed. For example, even where a patent is a continuing application under 35 U.S.C. 120, the effective date of some of the claims could be the filing date of the child application which resulted in the patent, because those claims were not supported in the parent application.

MPEP § 2617.

In the June 15, 2011 Office Action, the examiner considered the applicants' arguments that the Edery 086 patent could claim priority to provisional application U.S. Serial No. 60/030,639, but ultimately, the examiner correctly found that the applicants could not claim priority to the provisional application. June 15, 2011 Office Action at p. 2. The applicants later responded to the June 15, 2011 Office Action on other grounds but did not address the examiner's rejection of the applicants' claim to priority. Accordingly, the applicants failed to demonstrate that the Edery 086 patent could claim priority earlier than May 17, 2001. The applicants' failure to demonstrate the priority by itself establishes the Edery 086 priority date of not earlier than May 17, 2001. Requesters note that the June 15, 2011 Office Action listed the priority date of the 942 application as November 6, 1997 without any analysis. This alleged priority date is incorrect for the reasons set forth below.

Moreover, as illustrated below, although the Edery 086 patent attempts to claim priority to U.S. Patent Nos. 6,480,962 and/or 6,804,780, the claims of the Edery 086 patent are "not supported" in those specifications. *See* U.S. Patent Nos. 6,480,692 and 6,804,780. Accordingly, the applicable priority date for purposes of the invalidity analysis is not earlier than May 17, 2001.

The following portions of the Edery 086 patent (and the Edery 822 patent) were all "new matter" in CIP application No. 09/861,229:

- FIG. 1a
- FIG. 1b
- FIG. 1c
- FIG. 2
- FIG. 3
- FIG. 4
- FIG. 5
- FIG. 6a
- FIG. 6b
- FIG. 7a
- FIG. 7b
- FIG. 8
- FIG. 9
- FIG. 10a

- FIG. 10b
- FIG. 11
- FIG. 12a
- FIG. 12b and
- Col. 1:55 thru Col. 24:3

Consequently, all of the descriptions constitute new matter first introduced on May 17, 2001 with the filing of the Edery 822 patent. Similarly, all of the descriptions and claim limitations relating to the aforementioned, including appending the security profile data to the downloadable and transmitting the appended downloadable to a destination computer, are new matter first introduced on May 17, 2001 with the filing of the Edery 822 patent.

Because the claim scope depends on the newly added material, claims 1- 8, 17- 23, 31, 32, 35, 36, 39 and 41 may only receive the benefit of priority to the May 17, 2001 filing date. *See, e.g.*, *Waldemar Link, GmbH & Co. v. Osteonics Corp.*, 32 F.3d 556, 558 (Fed. Cir. 1994). Therefore, the Ji patent and the Touboul Application properly serve as prior art because their disclosures predate the priority date of the claimed subject matter of the Edery 086 patent.

IV. EXPLANATION OF PERTINENCE AND MANNER OF APPLYING CITED PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED UNDER 37 C.F.R. 1.510(B)(2)

A. The Ji Patent In View Of The Touboul Application

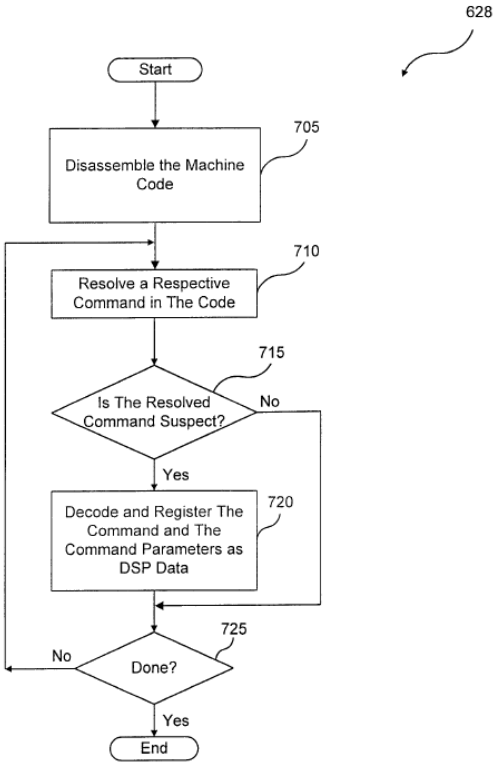
Claims 1- 8, 17- 23, 31, 32, 35, 36, 39 and 41 are obvious under 35 U.S.C. § 103(a) in light of Ji patent in view of the Touboul Application. The claim chart below details the manner of applying the Ji patent and Touboul Application to every claim of the Edery 086 patent for which reexamination is requested.

As discussed above, the Edery 086 patent is not entitled to a priority date earlier than May 17, 2001. The Ji patent was filed on September 10, 1997. The Touboul Application was filed on November 6, 1997. Accordingly, the combination of the Ji patent and the Touboul Application is prior art to the Edery 086 patent under 35 U.S.C. § 103(a).

Additionally, a person of ordinary skill would be motivated to combine the Ji patent with the teachings of the Touboul Application because the Touboul Application, like the Ji patent (at 1:3-6), is directed toward detecting and blocking computer viruses and other malicious code attacks. Touboul Application Abstract, 1:6-7.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
1. A computer-based method,	The Ji patent discloses the preamble. Ji discloses computer

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
comprising the steps of:	implemented applications executing on a computer network. Specifically, the Ji patent's Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;	The Touboul Application discloses deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable in Figure 7 and its related disclosure:

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	 FIG. 7 "FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a Downloadable into DSP data 310. Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step 710. Otherwise, if the code scanner 325 in step 715 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations,

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725." Touboul App. at 17:1-16. According to the Touboul Application, "[T]he code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code**.** It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker." Touboul App.at 9:14-24 (emphasis added). Thus, the Touboul Application discloses deriving security profile data for the Downloadable.
appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and	The combination of the Ji patent and the Touboul Application teaches or suggests the step of "appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable." The Ji patent discloses the "appending" claim element through its disclosure of appending, at the server, security monitoring package to the Java applet (Downloadable): "More broadly, the present invention is directed to delivering what is referred to as a "live agent" (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). *See also* Ji at 8:4-10 and 7:41-44. Therefore, the Ji patent discloses the appending of a security monitoring package to a Downloadable. And as described above, the Touboul Application discloses deriving

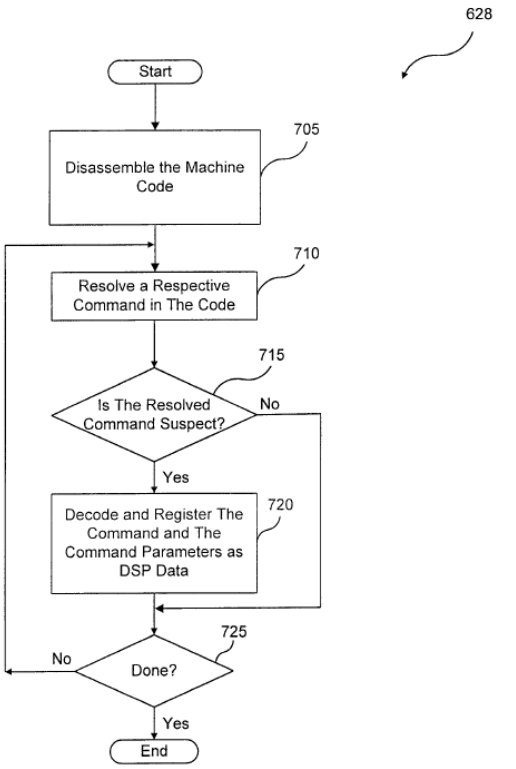
Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	downloadable security profile data. Touboul App. at Fig. 7, 17:1-16, 9:14-24. A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent showed awareness of Finjan Software, Ltd., the Touboul Application's applicant and assignee, by specifically disclosing Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by these software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, Ltd., a person of ordinary skill in the art would have been motivated to combine the Ji patent with the teachings of Finjan's Touboul Application to provide a solution balancing server-side and client-side activity. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
transmitting the appended Downloadable to a destination computer.	The Ji patent discloses the step of transmitting the applet, security monitoring package and the downloadable security profile data (appended Downloadable) to the destination computer. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the downloadable: "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). Ji additionally states, "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10 (emphasis added). Finally, Ji discloses that "The monitor package contains monitoring functions that are delivered from the server 32 to the client web browser 22 with the instrumental applet and are invoked by the instrumentation code in the applet." Ji at 7:41-44. As noted above, to achieve the load balancing objectives mentioned in Ji (1:66-2:42), a person of ordinary skill in the art would be motivated to combine the Ji patent with the Touboul Application's teaching of deriving the downloadable security profile ("DSP") data that is appended to the applet and monitoring package and transmitted to the client. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
2. The computer-based method of claim 1 wherein the Downloadable includes an applet.	The Ji patent discloses the method step wherein the Downloadable includes an applet. "Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server." Ji at 3:16-22 (emphasis added).
3. The computer-based method of claim 1 wherein the Downloadable includes an active control.	The Ji patent discloses the method step wherein the Downloadable includes an active control. "Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server." Ji at 3:16-22 (emphasis added).
4. The computer-based method of claim 1 wherein the Downloadable includes program script.	It would have been obvious to include scanning for program script (e.g., Java Script or Visual Basis script) to one of ordinary skill in the art because Java and Java Script are closely related. Moreover, it would have been obvious to combine the Ji patent with the teachings of the Touboul Application because the Touboul Application, like the Ji patent (1:6-7), is directed

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	toward detecting and blocking computer viruses and other malicious code attacks. Touboul Application; 2:7-18. The Touboul Application discloses, in addition to Java applets and ActiveX controls, the detection and prevention of both Java Script and Visual Basic attacks. Touboul Application at Abstract ("The Downloadable may include a Java™ applet. An ActiveX™ control, a JavaScript™ script, or a Visual Basic script.").
5. The computer-based method of claim 1 wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.	The Ji patent inherently discloses the method wherein the suspicious computer operations include calls made to an operating system, a file system, a network system and to memory. The Ji patent discloses a method that detects all suspicious instructions. The Ji patent discloses scanning the downloaded file to identify "suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server. Ji at 5:16-6:37 ("Examples of pre- and post-monitor functions are: (1) to disallow any directory listing access: pre-filter(function_name, parameters) { if (function_name = = "java.io.File.list") throw new SecurityException(); } post-filter(result) { }"). Accordingly, this instrumentation (deriving) identifies specific applet instructions deemed to be "suspicious" (computer operations) as determined by "a predefined set of [insecure] functions." Ji at 5:22-23. Moreover, during the instrumentation process, all potentially suspicious computer operations are identified and listed because the Ji patent discloses a process whereby all Java class files that may be called by the downloadable are scanned and instrumented: "An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once. A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	This creates a problem of how to maintain information on session states. To solve this problem, the pre-fetcher 38 pre-fetches the dependency class files during the static scanning of the main applet code module. The dependency class files are (see below) instrumented once, packed together, and delivered to the client." Ji at 7:8-28. Additionally, it would have been obvious to combine the teachings of the Ji patent with the Touboul Application. The Touboul Application discloses detecting suspicious computer instructions wherein the calls are made to an operating system, a file system, a network system, and to memory. Touboul Application at 17:13-16 ("The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds).")).
6. The computer-based method of claim 1 wherein the Downloadable security profile data includes a URL from where the Downloadable originated.	The Ji patent inherently discloses the method step wherein the downloadable security profile data includes a URL from there the downloadable originated. Because the applet (downloadable) is received by a HTTP proxy server with the URL of the originating web server included in the downloaded applet. The applet is subsequently scanned, instrumented and then sent to the web browser on the requesting client computer (see Fig. 1 of the Ji patent): "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8. Additionally, it would have been obvious to combine the teachings of the Touboul Application with the Ji patent to perform the method step wherein the downloadable security profile data includes a URL from where the downloadable originated. The Touboul Application discloses the inclusion of a URL as

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	part of the security profile data in claim 4: "The method of claim 1, further comprising the step of comparing the URL from which the Downloadable originated against a known URL." Touboul Application at 19:16-17. The Touboul Application also discloses a URL comparator in claim 57: "The system of claim 32. further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL." Touboul App. at 27:1-3.
7. The computer-based method of claim 1 wherein the appended Downloadable includes a digital certificate.	The Ji patent discloses the method step wherein the appended downloadable includes a digital certificate. As the specification discloses: "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10.
8. The computer-based method of claim 1 wherein said deriving Downloadable security profile data comprises disassembling the incoming Downloadable.	The Ji patent discloses the method step wherein the deriving of the suspicious instructions (downloadable security profile data) comprises disassembling the incoming applet (downloadable). The Ji patent discloses scanning the downloaded file to identify "suspicious instructions" (Ji at 5:22) contained in the downloadable as it is received at the server (as explained in detail in Ji at 5:16-6:37) requires disassembling the Java code in the applet to instrument the applet with pre- and post-filter interrupts. Additionally, it would have been obvious to combine the Ji patent with the teachings of the Touboul Application. The Touboul Application teaches disassembling the downloadable to derive the downloadable security profile data. Touboul Application at 17:2-3 ("Method 628 begins in step 705 with the code scanner 325 disassembling the machine code or the Downloadable.").
17. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation."

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and	The Touboul Application discloses deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable in Figure 7 and its related disclosure:  FIG. 7 "FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a

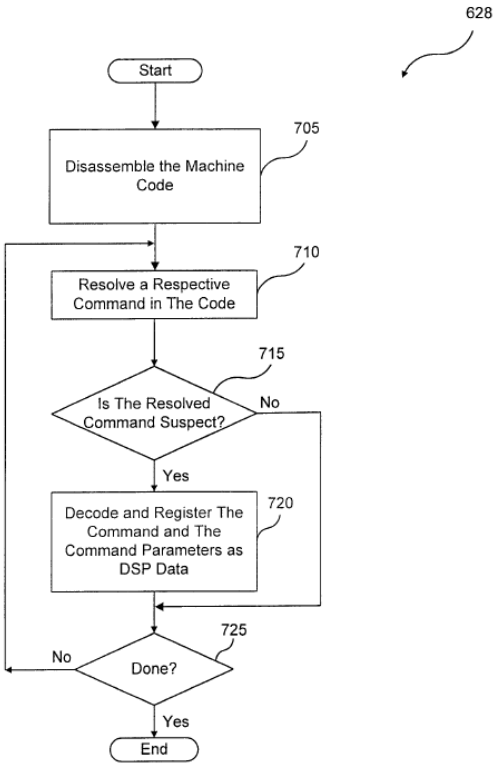
Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	Downloadable into DSP data 310. Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step 710. Otherwise, if the code scanner 325 in step 715 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725." - Touboul App. at 17:1-16. According to the Touboul Application, "[T]he code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. <u>The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code</u>**.** It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker." Touboul App. at 9:14-24 (emphasis added). Thus, the Touboul Application discloses deriving security profile data for the Downloadable.
transmitting the	The combination of the Ji patent and the Touboul Application

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.	teaches or suggests the step of "transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission." The Ji patent discloses the combined Downloadable and a representation of the Downloadable security profile data (the representation disclosed by the Touboul Application discussed below). The Ji patent discloses the Downloadable and the representation of the downloadable through its disclosure of appending, at the server, security monitoring package to the Java applet (Downloadable): "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). Ji additionally states, "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10 (emphasis added). Finally, Ji discloses that "The monitor package contains monitoring functions that are delivered from the server 32 to the client web browser 22 with the instrumental applet and are invoked by the instrumentation code in the applet." Ji at 7:41-44. Therefore, the Ji patent discloses the appending of a security monitoring package to a Downloadable. And as described above, the Touboul Application discloses deriving downloadable security profile data. Touboul App. at Fig. 7, 17:1-16, 9:14-24. The Ji patent also discloses the step of transmission via a transport protocol transmission through, for example, its disclosure of the Hypertext Transfer Protocol (HTTP). As shown in Figure 1 of the Ji patent, the scanner runs on the HTTP proxy server. And the instrumented applet is

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	downloaded from the HTTP proxy server to the requesting web browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8. A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent showed awareness of Finjan Software, Ltd., the Touboul Application's applicant and assignee, by specifically disclosing Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by these software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, Ltd., a person of ordinary skill in the art would have been motivated to combine the Ji patent with the teachings of Finjan's Touboul Application to provide a solution balancing server-side and client-side activity. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
18. The computer-based method of claim 17 wherein the transport protocol is an application transport protocol, and wherein the Downloadable security profile data is inserted as a header within the transport protocol transmission.	The Ji patent discloses the method step wherein the transport protocol is an application transport protocol, and wherein the Downloadable security profile data is inserted as a header within the transport protocol transmission. Regarding "the transport protocol is an application transport protocol" claim element, as explained in dependent claim 19, which depends from claim 18, HTTP is a transport application protocol. Accordingly, as shown in Figure 1 of the Ji patent,

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	the scanner runs on the HTTP proxy server. And the instrumented applet is downloaded from the HTTP proxy server to the requesting web browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8. Regarding the "downloadable security profile data is inserted as a header within the transport protocol transmission" claim element, the Ji patent inherently discloses this claim element because the URL (which is part of the downloadable security profile data as claimed by the Edery 086 patent in claim 6) is included in the header file. "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8.
19. The computer-based method of claim 18 wherein the application transport protocol is HTTP.	The Ji patent discloses the method step wherein the application transport protocol is HTTP. As shown in Figure 1 of the Ji patent, the scanner runs on the HTTP proxy server. And the instrumented applet is downloaded from the HTTP proxy server to the requesting web browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8.

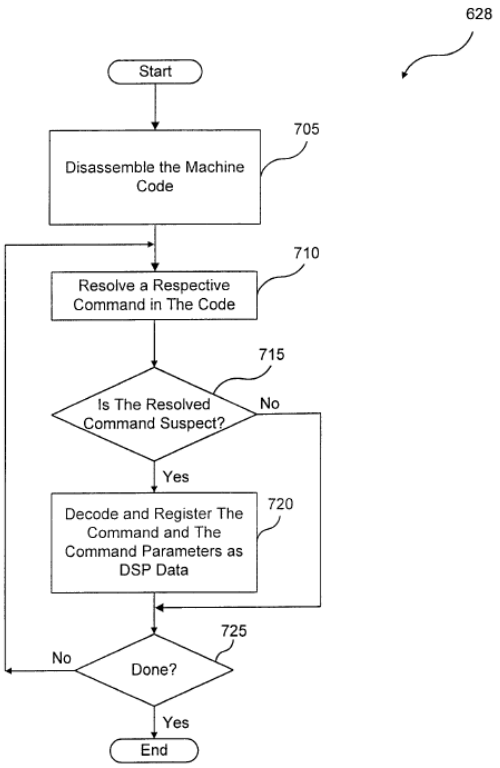
Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
20. The computer-based method of claim 18 wherein the application transport protocol is FTP.	The Ji patent inherently discloses the method step wherein the application transport protocol is FTP because the instrumented applet is downloaded to the requesting client computer's web browser. In addition to the HTTP protocol, web browsers support execution of the FTP protocol too.
21. The computer-based method of claim 17 wherein the transport protocol is a network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission.	The Ji patent inherently discloses the method step wherein the transport protocol is a network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission. Per dependent claim 22 (which depends from claim 21), TCP/IP is a network transport protocol. TCP/IP is a network protocol supported by the Windows and Linux operating systems. TCP/IP uses frames for transporting information. Accordingly, the downloadable security profile data must be transported via frames because all information transported using the TCP/IP protocol uses frames.
22. The computer-based method of claim 21 wherein the network transport protocol is TCP/IP.	The Ji patent inherently discloses the method step wherein the network transport protocol is TCP/IP. TCP/IP is a network protocol supported by the Windows and Linux operating systems.
23. The computer-based method of claim 21 wherein the network transport protocol is UDP.	The Ji patent inherently discloses the method step wherein the network transport protocol is UDP. As one of skill in the art at the time would have known, UDP is a network protocol supported by the Windows and Linux operating systems.
31. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Ji patent's Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	conventionally received from e.g. the Internet or an Intranet at a conventional server.").
receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;	The Touboul Application discloses receiving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable in Figure 7 and its related disclosure:  FIG. 7 "FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a Downloadable into DSP data 310. Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step 710.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	Otherwise, if the code scanner 325 in step 715 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725." Touboul App. at 17:1-16. According to the Touboul Application, "[T]he code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code**.** It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker." Touboul App. at 9:14-24 (emphasis added). Thus, the Touboul Application discloses deriving security profile data for the Downloadable.
appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and	The combination of the Ji patent and the Touboul Application teaches or suggests the step of "appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable." The Ji patent discloses the "appending" claim element through its disclosure of appending, at the server, security monitoring package to the Java applet (Downloadable): "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	instructions." Ji at 3:45-50 (emphasis added). *See also* Ji at 8:4-10 and 7:41-44. Therefore, the Ji patent discloses the appending of security monitoring package to a Downloadable. And as described above, the Touboul Application discloses deriving downloadable security profile data. Touboul App. at Fig. 7, 17:1-16, 9:14-24. A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent showed awareness of Finjan Software, Ltd., the Touboul Application's applicant and assignee, by specifically disclosing Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by these software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, Ltd., a person of ordinary skill in the art would have been motivated to combine the Ji patent with the teachings of Finjan's Touboul Application to provide a solution balancing server-side and client-side activity. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
transmitting the appended Downloadable to a destination computer.	The Ji patent discloses the step of transmitting the appended Downloadable to a destination computer via its disclosure of the applet, security monitoring package and the downloadable security profile data (appended Downloadable) to the destination computer. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the downloadable: "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g.

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). Ji additionally states, "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10 (emphasis added). Finally, Ji discloses that "The monitor package contains monitoring functions that are delivered from the server 32 to the client web browser 22 with the instrumental applet and are invoked by the instrumentation code in the applet." Ji at 7:41-44. As noted above, to achieve the load balancing objectives mentioned in Ji (1:66-2:42), a person of ordinary skill in the art would be motivated to combine the Ji patent with the Touboul Application's teaching of deriving the downloadable security profile ("DSP") data that is appended to the applet and monitoring package and transmitted to the client. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
32. The computer-based method of claim 31 further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data.	The Ji patent discloses the method step comprising forwarding the downloadable to an external computer for deriving the downloadable security profiled data. Specifically, the Ji patent discloses for Figure 1 that "[t]he security policy generator 54 may run on server machine 20 or another computer." Ji at 7:53-55 (emphasis added).
35. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation."

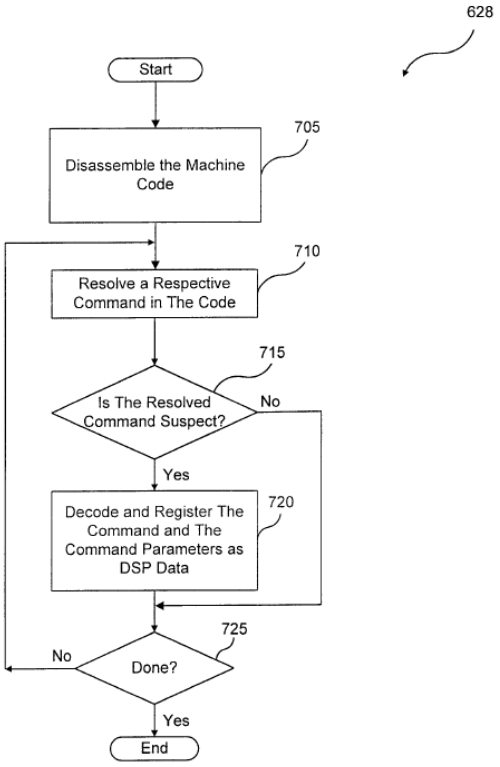
Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and	The Touboul Application discloses receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable in Figure 7 and its related disclosure:  FIG. 7 "FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a Downloadable into DSP data 310. Method 628 begins in step

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step 710. Otherwise, if the code scanner 325 in step 715 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725." Touboul App. at 17:1-16. According to the Touboul Application, "[T]he code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker." Touboul App. at 9:14-24 (emphasis added). Thus, the Touboul Application discloses deriving security profile data for the Downloadable.
transmitting the Downloadable and a	The combination of the Ji patent and the Touboul Application teaches or suggests the step of "transmitting the Downloadable

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.	and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission." The Ji patent discloses the combined Downloadable and a representation of the Downloadable security profile data (the representation disclosed by the Touboul Application discussed below). The Ji patent discloses the Downloadable and the representation of the downloadable through its disclosure of appending, at the server, security monitoring package to the Java applet (Downloadable): "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). Ji additionally states, "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10 (emphasis added). Finally, Ji discloses that "The monitor package contains monitoring functions that are delivered from the server 32 to the client web browser 22 with the instrumental applet and are invoked by the instrumentation code in the applet." Ji at 7:41-44. Therefore, the Ji patent discloses the appending of a security monitoring package to a Downloadable. And as described above, the Touboul Application discloses deriving downloadable security profile data. Touboul App. at Fig. 7, 17:1-16, 9:14-24. The Ji patent also discloses the step of transmission via a transport protocol transmission through, for example, its disclosure of the Hypertext Transfer Protocol (HTTP). As shown in Figure 1 of the Ji patent, the scanner runs on the HTTP proxy server. And the instrumented applet is downloaded from the HTTP proxy server to the requesting web

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8 A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent showed awareness of Finjan Software, Ltd., the Touboul Application's applicant and assignee, by specifically disclosing Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by these software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, Ltd., a person of ordinary skill in the art would have been motivated to combine the Ji patent with the teachings of Finjan's Touboul Application to provide a solution balancing server-side and client-side activity. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
36. The computer-based method of claim 35 further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data.	The Ji patent discloses the method step comprising forwarding the downloadable to an external computer for deriving the downloadable security profiled data. Specifically, the Ji patent discloses for Figure 1 that "[t]he security policy generator 54 may run on server machine 20 or another computer." Ji at 7:53-55 (emphasis added).
39. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for

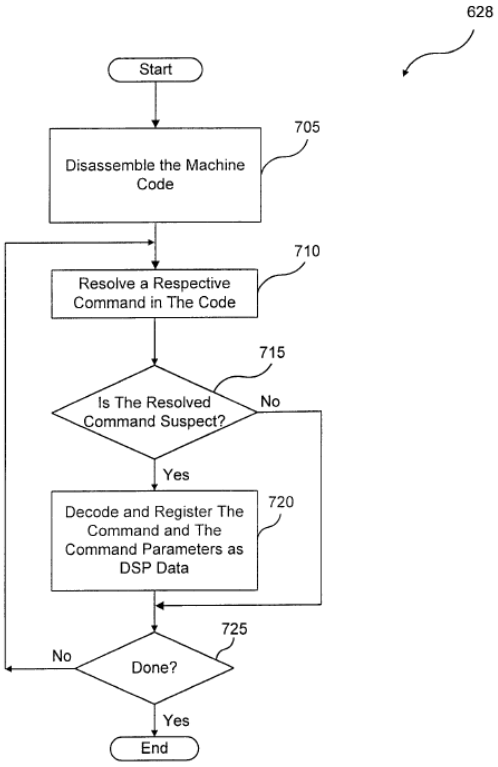
Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").
retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable;	The Touboul Application discloses retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable in Figure 7 and its related disclosure:

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	 FIG. 7 "FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a Downloadable into DSP data 310. Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step 710. Otherwise, if the code scanner 325 in step 715 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations,

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725." Touboul App. at 17:1-16. According to the Touboul Application, "[T]he code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code**.** It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker." Touboul App. at 9:14-24 (emphasis added). Thus, the Touboul Application discloses deriving security profile data for the Downloadable.
appending a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and	The combination of the Ji patent and the Touboul Application teaches or suggests the step of "appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable." The Ji patent discloses the "appending" claim element through its disclosure of appending, at the server, security monitoring package to the Java applet (Downloadable): "More broadly, the present invention is directed to delivering what is referred to as a "live agent" (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). *See also* Ji at 8:4-10 and 7:41-44. Therefore, the Ji patent discloses the appending of a security monitoring package to a Downloadable. And as described above, the Touboul Application discloses deriving downloadable security profile data. Touboul App. at Fig. 7,

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	17:1-16, 9:14-24. A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent specifically discloses Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by the software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, LTD, a person of ordinary skill in the art would have been motivated to combined the Ji patent with the teachings of Finjan's Touboul Application. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
transmitting the appended Downloadable to a destination computer.	The Ji patent discloses the step of transmitting the applet, security monitoring package and the downloadable security profile data (appended Downloadable) to the destination computer. The Ji patent explains that, as depicted in Fig. 1, the security monitoring package and security policies are included with the downloadable: "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). Ji additionally states, "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10 (emphasis added). Finally, Ji discloses that "The monitor package contains monitoring functions that are delivered from the server 32 to the client web browser 22 with the instrumental applet and are invoked by the instrumentation code in the applet." Ji at 7:41-44. As noted above, to achieve the load balancing objectives mentioned in Ji (1:66-2:42), a person of ordinary skill in the art would be motivated to combine the Ji patent with the Touboul Application's teaching of deriving the downloadable security profile ("DSP") data that is appended to the applet and monitoring package and transmitted to the client. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.
41. A computer-based method, comprising the steps of:	The Ji patent discloses the preamble. Ji discloses computer implemented applications executing on a computer network. Specifically, the Abstract discloses a "network scanner for security checking of application programs […] received over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. […] During run time at the client, the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation." Figure 1 of the Ji patent discloses a server and client computer device. It is well understood that a computer includes one or more processors for executing software applications.
receiving an incoming Downloadable;	The Ji patent discloses the step of receiving an incoming downloadable. The Ji patent discloses receiving files "(e.g. Java applets or ActiveX controls)" from the Internet at the server in Fig. 1. See also Ji patent at 3:17-23 ("Thereby in accordance with the invention a scanner (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the Internet or an Intranet at a conventional server.").

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and	The Touboul Application discloses retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable in Figure 7 and its related disclosure:  FIG. 7 "FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a Downloadable into DSP data 310. Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	710. Otherwise, if the code scanner 325 in step 715 determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725." Touboul App. at 17:1-16. According to the Touboul Application, "[T]he code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code**.** It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker." Touboul App. at 9:14-24 (emphasis added). Thus, the Touboul Application discloses deriving security profile data for the Downloadable.
transmitting the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.	The combination of the Ji patent and the Touboul Application teaches or suggests the step of "transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission." The Ji patent discloses the combined Downloadable and a representation of the Downloadable security profile data (the representation disclosed by the Touboul Application discussed below). The Ji patent discloses the Downloadable and the representation of the downloadable through its disclosure of appending, at the server, security monitoring package to the

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	Java applet (Downloadable): "More broadly, the present invention is directed to delivering what is referred to as a 'live agent' (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the monitoring package being intended to prevent execution of the suspicious instructions." Ji at 3:45-50 (emphasis added). Ji additionally states, "Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package. The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution." Ji at 8:4-10 (emphasis added). Finally, Ji discloses that "The monitor package contains monitoring functions that are delivered from the server 32 to the client web browser 22 with the instrumental applet and are invoked by the instrumentation code in the applet." Ji at 7:41-44. Therefore, the Ji patent discloses the appending of a security monitoring package to a Downloadable. And as described above, the Touboul Application discloses deriving downloadable security profile data. Touboul App. at Fig. 7, 17:1-16, 9:14-24. The Ji patent also discloses the step of transmission via a transport protocol transmission through, for example, its disclosure of Hypertext Transfer Protocol (HTTP). As shown in Figure 1 of the Ji patent, the scanner runs on the HTTP proxy server. And the instrumented applet is downloaded from the HTTP proxy server to the requesting web browser on the client machine: "Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software 26. (Downloaded non-applets are not scanned.) The instrumented applet is subject to a special digital signer which is an (optional) part of the scanner 26. The scanned (instrumented) applet, which has been digitally signed is then downloaded to the web browser 22 in the client 14." Ji at 4:66-5:8

Edery 086 Patent Claim Limitations	The Ji Patent in View of the Touboul Application
	A person of ordinary skill in the art would have been motivated to combine the teachings of the Ji patent and Touboul Application because the disclosures cover similar technology in seeking to prevent the execution of potentially harmful computer malware by the requesting client computer. Moreover, the Ji patent showed awareness of Finjan Software, Ltd., the Touboul Application's applicant and assignee, by specifically disclosing Finjan's SurfinGate and SurfinShield anti-malware software products as server-side and client-side applications, respectively. Ji patent at 1:66-2:42 (SurfinGate performs static scanning on the server and SurfinShield performs run-time monitoring on the client). The Ji patent concludes that a combination of server-side and client-side processing offered by these software products is required "[t]o distribute the load between the server and client evenly." Ji patent at 2:62-3:4. And because the applicant for the Touboul Application was Finjan Software, Ltd., a person of ordinary skill in the art would have been motivated to combine the Ji patent with the teachings of Finjan's Touboul Application to provide a solution balancing server-side and client-side activity. Thus, the combination of the Ji patent and the Touboul Application teaches or suggests this limitation.

V. CONCLUSION

Based on the above remarks, it is respectfully submitted that a substantial new question of patentability has been raised with respect to claims 1-8, 17- 23, 31, 32, 35, 36, 39 and 41 of the Edery 086 patent. Therefore, reexamination of claims 1-8, 17- 23, 31, 32, 35, 36, 39 and 41 is respectfully requested.

Respectfully submitted,

Dated: February 7, 2014

/Ryan W. Cobb/
Ryan W. Cobb
Reg. No. 64,598
Attorney for Requestor

DLA PIPER LLP (US)
401 B Street, Suite 1700
San Diego, CA 92101
ryan.cobb@dlapiper.com
(619) 699-2700
(619) 699-2701